ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ТА ЕКОНОМІЧНА БЕЗПЕКА

УДК 338.28:355.45:004.738.5 **DOI: 10.37332/2309-1533.2021.3-4.23**
JEL Classification: L86, M15

Ревак І.О.,
д-р екон. наук, професор,
професор кафедри соціально-гуманітарної підготовки,
Грень Р.Т.,
аспірант* кафедри соціально-гуманітарної підготовки,
Львівський державний університет внутрішніх справ

ОСОБЛИВОСТІ ФОРМУВАННЯ БЕЗПЕЧНОГО КІБЕРПРОСТОРУ В УМОВАХ РОЗВИТКУ ЦИФРОВОЇ ЕКОНОМІКИ

Revak I.O.,
dr.sc.(econ.), professor, professor at the department of social and humanitarian training,
Gren R.T.,
postgraduate student at the department of social and humanitarian training,
Lviv State University of Internal Affairs

PECULIARITIES OF THE FORMATION OF SECURE CYBERSPACE IN THE DIGITAL ECONOMY

Постановка проблеми. Розвиток цифрової економіки у сучасному світі спрямований на створення та об'єднання комунікативного суспільства, забезпечення соціального зростання інформаційних платформ та стартапів, конверсію фінансової інфраструктури, прискорення грошових транзакцій, цифровізацію адміністративно-цивільних послуг тощо.

Технології електронної ідентифікації особи, блокчейн, електронний банкінг наповнюють сучасне економічне життя новим призначенням, базисом якого виступають нові знання та підготовлені фахівці. На сьогодні нормативна база не може гарантувати належний рівень боротьби з інформаційними злочинами, тому кількість злочинів в сфері ІТ зростає. На нашу думку, необхідно налагодити взаємозв'язки у середовищі віртуального світу, щоб суспільно передові цифрові технології запобігали проявам недобросовісної конкуренції та випереджували вірогідність майбутніх втрат.

Аналіз останніх досліджень і публікацій. Наукові праці багатьох дослідників висвітлюють проблематику моніторингу цифрових процесів, виявлення загроз інформаційній та кібербезпеці, захисту інформаційного простору від кібератак та кібертероризму. Зокрема, цим питанням присвячені праці В. Бурячка, Д. Дубова, М. Ожевана, В. Толубка, В. Хорошка та ін. Окремі дослідження торкаються питань цифрової економіки, розвитку цифрових технологій та інфраструктури. Так, В. Ляшенко та О. Вишневський розглядають цифрову модернізацію національної економіки в якості проривного розвитку. І. Носатов визначає шляхи розвитку інформаційних технологій у розрізі стратегічних трансформаційних змін [6]; Н. Пантєлєєва досліджує системоутворюючі чинники виникнення кіберзагроз в умовах цифровізації національної економіки [8]. На інноваційному розвитку та реалізації стратегії цифровізації економіки з урахуванням світових трендів щодо інвестицій в сучасні технології залежно від сектора та реалізованої бізнес-моделі наголошує І. Плікус [9]; основні засади цифровізації секторів економіки (первинного, вторинного, третинного, четвертинного) з акцентом на сферу інноваційних технологій та природних ресурсів обґрунтовують Т. Гірченко, Г. Чмерук, І. Семенюк [2]. Натомість, малодослідженими залишаються питання формування

* *Науковий керівник: Ревак І. О. - д-р екон. наук, професор.*

безпечного кіберпростору в умовах розвитку цифрової економіки, боротьби з «цифровою злочинністю» тощо.

Постановка завдання. Метою статті є розкриття особливостей формування безпечного кіберпростору в умовах розвитку цифрової економіки, обґрунтування напрямів діяльності правоохоронних органів щодо запобігання кіберзлочинності.

Виклад основного матеріалу дослідження. Тенденції розвитку сучасної цивілізації сигналізують про те, що інформаційні технології не розвиваються окремо від культурних і соціальних потреб людства. Зростання масштабів впровадження комп'ютерних технологій та кількості користувачів мобільних пристроїв, підключених до інтернету, одночасно зі створенням нових просторів спілкування, посилюють техногенні загрози і створюють правовий вакуум, яким можуть користуватися зловмисники. Проте, не дивлячись на супутні ризики, сучасний рівень розвитку інформаційно-комунікаційних технологій дає можливість створити єдиний глобальний комунікаційний простір, в якому можна виробити загальні норми, узгоджувані з цінностями різних національних культур.

Ключові моменти щодо використання інформаційно-комунікаційних та цифрових технологій в економічних процесах, стимулювання внутрішнього ринку виробництва та створення конкурентоспроможного національного товаровиробника, введення відповідних стимулів для цифровізації національної економіки закладені в основу Концепції розвитку цифрової економіки та суспільства України на 2018–2020 роки [5]. Безумовно, Україна має потенціал розвитку цифрової індустрії, оскільки ця галузь є однією з найбільш прибуткових та перспективних з точки зору вкладення капіталу. Новітня модель цифрової трансформації економіки пов'язана з розвитком бізнес-стартапів, які використовують цифрові платформи, відтак постійно еволюціонують та вдосконалюються. Особливістю цифрових платформ є об'єднання різних груп споживачів, виробників, власників ресурсів в одному віртуальному просторі. Варто зауважити, що вітчизняний цифровий капітал перебуває на стадії формування, однак можна назвати чимало прикладів реалізації успішних проєктів. Безумовно можливості розвитку цифрової економіки в Україні пов'язані з розширенням використання цифрових платформ, зокрема технології блокчейн.

З урахуванням особливостей цифровізації економіки до характеристик кіберпростору, на нашу думку, можна віднести:

– специфічні фізичні властивості: інформаційний простір без проблем долає фізичні перепони і географічну віддаленість;

– особливі часові характеристики, пов'язані з тим, що комунікація в них є практично миттєвою;

– мінливість, обумовлена безперервними змінами інтернет-конфігурацій під впливом змін в потоках інформації;

– проникність в умовах правових обмежень і юрисдикції.

Бурхливий розвиток інформаційних технологій актуалізує питання забезпечення інформаційної та кібернетичної безпеки, при цьому головними проблемами можна вважати відсутність чіткого розуміння ключової ролі кібербезпеки у зміцненні національної безпеки держави, законодавча неврегульованість на рівні понятійно-категорійного апарату; дефіцит методичного забезпечення та розробки практичних рекомендацій; неузгодженість дій з боку державних органів щодо створення автономних підрозділів системи кібербезпеки. На практиці кібербезпека спрямована насамперед на ті типи атак, зломів чи інцидентів, які є цільовими, складними для виявлення або управління.

Стандарт ISO / IEC 27032 визначає кібербезпеку як різновид безпеки інтерактивного інформаційного середовища, що дає можливість зберігати конфіденційність, цілісність та доступність інформації у віртуальному середовищі. У цьому випадку кіберпростір є результатом функціонування на основі загальних принципів та правил інформаційно-комунікаційних систем зв'язку [13]. Згідно ДСТУ ISO/IEC 27032:2016, кіберпростір – це складне інтерактивно інформаційне середовище, що виникає та функціонує внаслідок кооперації людей, комп'ютерних систем, Інтернет-послуг та діє завдяки інтегрованим мережам і технічним обладнанням [3].

На відміну від інформаційної безпеки, кібербезпека – це не лише захист самого кіберпростору, а й захист тих, хто функціонує в кіберпросторі, та будь-якого їхнього майна, що можна отримати через кіберпростір. Кібербезпека – це захист інформаційних активів шляхом усунення загроз для інформації, що обробляється, зберігається і переданої між мережевими інформаційними системами.

Прийнята 2016 року Стратегія кібербезпеки України сфокусована на створення умов для безпечного функціонування кіберпростору, формування національної системи кібербезпеки, забезпечення ефективної боротьби з кіберзагрозами, кібершпигунством, кібертероризмом, організацію кіберзахисту державних електронних інформаційних ресурсів, інформаційної інфраструктури, зокрема критичної [10].

З урахуванням результатів багатокритеріального аналізу, колектив авторів [1, с. 10] під кіберпростором розуміє віртуальне комунікаційне середовище, утворене системою взаємозв'язків між користувачами та об'єктами інформаційної інфраструктури. Натомість офіційні джерела деяких країн Євросоюзу до кіберпростору зараховують віртуальний простір, в якому обертаються електронні дані усіх ПК, або всі форми мережевої цифрової діяльності, зокрема їх зміст та дії, що проводяться через

цифрові мережі, або ж усі елементи інформаційної інфраструктури, доступні в мережі Інтернет, опускаючи будь-які територіальні кордони [11; 12].

Фахівці з інформаційних технологій виділяють кілька хвиль розвитку цифрових технологій, кожна з яких характеризується технічним прогресом та низкою загроз. Перша хвиля включає впровадження інформаційно-комунікаційних технологій, комп'ютеризацію ключових сфер діяльності, автоматизацію процесів управління (включаючи впровадження і використання ERP, EDI, CRM тощо) та впровадження широкосмугового доступу. Друга хвиля характеризується розробкою та впровадженням онлайн-платформ, таких як пошукові системи, торгові платформи, дистанційне навчання та соціальні мережі. Третя хвиля передбачає впровадження таких технологій, як прогнозний аналіз великих даних, промисловий Інтернет або Інтернет речей, робототехніка, адитивні технології (включаючи 3D-друк) та штучний інтелект (включаючи машинне навчання).

Основна увага в кібербезпеці пов'язана з розробкою та впровадженням ефективних засобів контролю, які допоможуть захистити підприємства та приватних осіб від навмисних атак, порушень, інцидентів та наслідків. Проблема налагодження відносин у віртуальному просторі полягає в тому, що це, головним чином, простір доменних імен IP-адрес. Водночас, сучасне суспільство характеризує інтернет-економіку як електронну комерцію із застосуванням новітніх електронних ресурсів. При цьому слід пам'ятати, що розвиток цифрових технологій посилює зростання тіньової економіки, оскільки з появою сучасних технологій можливість «цифрових злочинів» зростає. З огляду на поширення міжнародних злочинів у віртуальному середовищі, важливим питанням є вплив цифрової економіки на світогосподарські процеси.

Кіберзлочинність, як і кібервійна, є новою формою деструктивних процесів, відтак злочином є протиправне діяння, передбачене законодавством, що тягне за собою покарання. Кіберзлочинність – це злочини, вчинені у віртуальному світі, через кіберпростір або проти інтернет простору. До такого виду загроз відносимо незаконне отримання, розголошення чи витік інформації, незаконне внесення змін до даних, неналежне використання обладнання, створення, використання та розповсюдження небезпечних програм, несанкціонований доступ до інформації, поширення розсилок тощо. Безперечно будь-які зловживання та дії зловмисників в інтернеті ще більше актуалізують питання національної безпеки, людської гідності, конфіденційності, репутації, захисту прав інтелектуальної власності.

Одним із ключових завдань управління безпекою в інтернет просторі є розробка та впровадження технологій захисту та протидії від атак у віртуальному середовищі. Відповідно до звіту Європолу «Оцінка ризиків організованої злочинності у віртуальному середовищі (IOCTA)» (2018) [6], правоохоронні органи в інтернет просторі повинні посилити роботу з виявлення і пошуку окремих злочинців і злочинних груп. Головним чином ініціюється створення національних і міжнародних баз даних про кіберзлочинність з використанням принципів кримінології, що є частиною сучасної «Європейської субкультурної злочинності». Тактичний звіт «IOCTA» надає ключові настанови правоохоронним органам, політикам та регуляторним органам щодо дієвої боротьби зі злочинами в інтернет просторі. Для того, щоб правоохоронні органи ефективно протидіяли злочинам в кіберпросторі, важливо забезпечити достатню кількість ресурсів для дослідження нових бізнес-технологій, розробку відповідного програмного забезпечення, доступ до багатоканальних джерел інформації. Правоохоронним органам необхідно володіти засобами, технікою та мати практичні навички протидії злочинам, що пов'язані з кодуванням та використанням режиму «інкогніто», VPN режиму (зашифроване підключення). Сьогодні компанії із запобігання інтернет злочинам переважно зосереджують увагу на потенційних жертвах (громадянах та бізнесі) у віртуальному середовищі. Окрім цього, необхідно посилити співпрацю з ймовірними хакерами, особливо з категорією неповнолітніх та молодих осіб, які мають певні навики в програмуванні.

Варто наголосити, що реальні кіберінциденти відбуваються не через якусь «аварію» чи «несприятливі обставини», а через неякісне управління інформаційними системами та недостатній рівень компетентності у сфері кібербезпеки. Оскільки кожна інформаційна система має безліч вбудованих засобів управління ІТ, які забезпечують її безперебійну, точну, надійну та ефективну роботу, застосування ефективніших базових та розширених засобів контролю сприятиме швидшому виявленню та запобіганню кіберзагрозам. Безперечно, для успішного управління кіберризиками дуже важливо постійно оцінювати ефективність засобів контролю безпеки. Про підвищену увагу до системи раннього сповіщення про кіберінциденти і розбудову Єдиної загальнодержавної системи протидії кіберзлочинності наголошують Д. Дубов та М. Ожеван [4, с. 30].

Вивчаючи зростання ІТ-ринку в Україні, окремі дослідники наголошують на економічних, соціальних та політичних факторах, які сприяють розвитку цифрової економіки. За результатами когнітивного моделювання до основних факторів віднесено: національну валюту, інтеграційний процес з Європейським союзом, заробітну плату та законодавчу базу [7, с. 163].

Проблемою виявлення загроз в даній області виступає те, що хакерські атаки стають пролонгованими в часі та можуть тривати місяцями, перш ніж їх виявлять. Еволюція таких атак веде до зміни стратегії протидії хакерам: якщо раніше заходи із забезпечення інформаційної безпеки передбачали виявлення і запобігання, то тепер вони все більше спрямовані на захист державних об'єктів. Прогрес у використанні інформаційно-комунікаційних технологій робить критичну

інфраструктуру менш вразливою до кібератак. Передумовами загострення проблем інформаційної безпеки на об'єктах критичної інфраструктури є перехід на автоматичний контроль обробки спеціалізованими процесами на критично важливих об'єктах; практика підключення офісних і промислових корпоративних мереж до інтернету; поширення мобільних пристроїв серед співробітників, що сприяє поширенню принципу «приноси свій пристрій»; ускладнення ланцюжків поставок і систем управління та контролю.

Аналізуючи характер та особливості вчинення інформаційних злочинів, варто окреслити такі важливі моменти:

1. Надмірна особиста та суспільна відкритість до віртуального світу. Злочини з використанням інформаційно-комунікаційних мереж та інновацій, як правило, є зручним сегментом для зловживань у міжнародній торгівлі, постачанні послуг, відмиванні грошей, грошових переказів між громадянами та підприємствами, використання хмарних технологій в інтернет просторі та підключенні комп'ютера до інтернет мереж.

2. Інноваційність. З швидким розвитком цифрових технологій виникає неузгодженість законодавчого характеру, а з урахуванням вітчизняних реалій – і корупційне лобіювання прийняття відповідних рішень щодо заходів з протидії злочинам в інтернет просторі.

3. Витончений характер злочинів. Хакери, які отримують матеріальну вигоду від кіберзлочинів, застосовують цифрові та передові технології, інформаційно-комунікаційні мережі з соціальних та психологічних причин. Це стосується, насамперед, наклепів на керівництво країни, розробки терористичних веб-сайтів, знищення інформаційних систем за допомогою введення вірусів або остаточне припинення функціонування таких систем (як додаток до форм тероризму, інформаційних війн).

4. Злочини інкогніто. Хакерів зацікавлює відсутність фізичного контакту з жертвою, порівняно пом'якшений вид покарання в деяких державах та труднощі розкриття, запису та отримання криміналістично важливої інформації в кіберпросторі.

5. Міжнародний характер та поширеність злочинів. За допомогою інформаційно-комунікаційних мереж підготовка та виконання кіберзлочину може реалізовуватись без часових та територіальних обмежень. Оскільки цифрові технології та веб-послуги стають загальнодоступними для суспільства, кількість злочинів у віртуальному середовищі невпинно зростає.

Наголошуючи на поширенні інтернет-злочинів у віртуальному середовищі, спробуємо їх класифікувати за такими видами:

– злочини, пов'язані з привласненням матеріальних активів;

– шахрайство та маніпулювання інформаційно-комунікаційними технологіями (для особистого використання або продажу);

– переривання діяльності інформаційно-комунікаційних систем задля одержання матеріальної вигоди та доступу до автоматичного контролю обробки (за сплачені умисно завдані збитки або шкоду опонентам);

– інші злочини в кіберпросторі.

Питання забезпечення правопорядку у кіберпросторі посилюють намагання представників корпоративного сектору в деяких країнах ЄС встановити тісні зв'язки щодо розробки заходів з протидії транснаціональній злочинності. Така взаємодія будується за певними напрямами. По-перше, бізнес-структури замовляють послуги у кіберзлочинців, зокрема щодо крадіжок інтелектуальної власності та компрометуючої конкурентів документації. По-друге, організовані злочинні угрупування інвестують отримані прибутки в легальний бізнес та ІТ-індустрію, особливо у фінансові технології, виготовлення відеоігор і різного роду мобільних додатків, які передбачають отримання від клієнтів персональних даних [8].

З метою надійного захисту кіберпростору використовуються новітні технологічні розробки. Так, двохфакторна верифікація розповсюджена зараз у хмарній електронній пошті (наприклад Gmail, Ukr.net) і стає все більш поширеною у роздрібному та інтернет-банкінгу; кіберрозвідка та аналіз є технічними інструментами підвищеного інтересу до «обміну інформацією» та «аналізу загроз». Уникнення таких загроз на нанорівні, як фішингові атаки, крадіжка особистої інформації та недопущення кіберінцидентів на національному і державному рівнях, на наш погляд, є пріоритетними напрямами зміцнення кібербезпеки.

Діяльність правоохоронних органів щодо недопущення (мінімізації, нейтралізації) реальних та потенційних загроз повинна охоплювати:

– тривале й стійке ефективне комунікативне співробітництво та тісний зв'язок між різними підрозділами органів внутрішніх справ та іншими державними структурами;

– діяльність різних відомств та підвідомчих правоохоронних органів в сфері інформаційних технологій для колективного функціонування та узгодження мети;

– інтенсивніше використання (застосування) електронних доказів, інформаційно-телекомунікаційних технологій та реєстрів;

– розробку критеріїв щодо регулювання таємних даних про ефективні обставини, установивши програмний доступ різних органів внутрішніх справ, які б ефективно протидіяли злочинам в цифрових комп'ютерних технологіях та кіберпросторі.

З огляду на те, що основною метою діяльності правоохоронних органів є боротьба з дилерами шкідливих цифрових послуг та відповідних інструментів, доцільним є створення реєстру таких постачальників, які мають сумнівну репутацію, в тому числі ІТ-компаній, інших суб'єктів господарювання, тим самим забезпечивши контроль над ситуацією у сфері цифрової економіки. Основними напрямами зміцнення кіберпростору можна вважати: безперервну модернізацію інформаційно-телекомунікаційних технологій; зміцнення комунікаційного захисту, а саме удосконалення, розробка та запуск новітніх програм охорони відомостей; нормативно-правову урегульованість та узгодження дій щодо створення окремих елементів системи кібербезпеки; запровадження та використання технології блокчейн.

Висновки з проведеного дослідження. Таким чином, цифрові комп'ютерні технології інтенсивно удосконалюються та набувають широкого попиту у всіх суспільних відносинах, бізнес-процесах, управлінській діяльності. Сьогодні Україна має унікальну можливість зробити «цифровий стрибок» у пріоритетних сферах економіки, розвивати цифрову інфраструктуру, сектор інформаційно-комунікаційних технологій, що дозволить не лише збільшити кількість робочих місць, а й забезпечити приріст ВВП. Створення нових сегментів прискорить розвиток приватного бізнесу та промисловості, а в сфері соціально-публічного управління – надання високоякісних публічних та соціальних послуг.

Спільними зусиллями держави та бізнес-структур цифровий розрив у наявності відповідних технологій та систем управління у різних секторах економіки можна подолати шляхом:

1) реалізації комплексної національної політики оцифрування;
2) створення попиту на якісні послуги, засновані на цифрових технологіях;
3) доступу до швидкісного Інтернету та максимальних можливостей для ведення бізнесу за допомогою цифрових технологій;
4) розвитку інфраструктури та взаємозв'язку цифрових послуг у всіх сферах.

Безперечно, швидка цифровізація національної економіки можлива завдяки функціонуванню безпечного кіберпростору. На порядок денний виходять питання створення вітчизняної нормативно-правової бази, розробки термінологічного апарату у цій сфері, приведення у відповідність до міжнародних стандартів і стандартів ЄС та НАТО вітчизняних нормативних документів у сфері електронних комунікацій, захисту інформації, інформаційної та кібербезпеки. Чималу увагу слід приділити створенню системи незалежного аудиту інформаційної безпеки, кіберзахисту об'єктів критичної інфраструктури, узгодженню використання спецзасобів структурними підрозділами, що відповідають за безпеку кіберпростору в Україні.

Література

1. Бурячок В. Л., Толубко В. Б., Хорошко В. О., Толюпа С. В. Інформаційна та кібербезпека: соціотехнічний аспект : підручник. Київ : ДУТ, 2015. 288 с.

2. Гірченко Т. Д., Чмерук Г. Г., Семенюк І. М. Шляхи модернізації цифрової економіки. *Інфраструктура ринку*. 2020. Вип. 41. С. 25-30.

3. ДСТУ ISO/IEC 27032:2016 (ISO/IEC 27032:2012, IDT) «Інформаційні технології. Методи захисту. Настанови щодо кібербезпеки». 27.12.2016. № 448. URL: http://online.budstandart.com/ua/catalog/doc-page.html?id_doc=69128 (дата звернення: 06.03.2021).

4. Дубов Д. В., Ожеван М. А. Кібербезпека: світові тенденції та виклики для України. Київ : НІСД, 2011. 30 с.

5. Концепція розвитку цифрової економіки та суспільства України на 2018-2020 роки : Розпорядження Кабінету Міністрів України від 17 січня 2018 № 67-р. URL: https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80#Text (дата звернення: 06.03.2021).

6. Ляшенко В. І., Вишневський О. С. Цифрова модернізація економіки України як можливість проривного розвитку : монографія. Київ, 2018. 252 с.

7. Носатов І. К. Шляхи розвитку інформаційних технологій в контексті стратегічної розбудови національної економіки. *Науковий вісник Херсонського державного університету. Серія: Економічні науки*. 2017. Випуск 22. Частина 2. С. 160-164.

8. Пантєлєєва Н. М. Кіберзагрози в умовах цифрової економіки. *Фінансовий простір*. 2019. № 1. С. 130-139.

9. Плікус І. Й. Цифрова економіка: ключові тренди в світі та перспективи для України. *Молодий вчений*. 2019. № 12. С. 470-476.

10. Стратегія кібербезпеки України : Указ Президента України від 15 березня 2016 року № 96/2016. URL: https://zakon.rada.gov.ua/laws/show/96/2016#Text (дата звернення: 06.03.2021).

11. Cyber Security Strategy for Germany 2016. URL: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-

security-strategy-for-germany/@@download_version/5f3c65fe954c4d33ad6a9242cd5bb448/file_en (дата звернення: 06.03.2021).

12. Cyber Security Strategy of the United Kingdom: safety, security and resilience in cyber space. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/228841/7642.pdf (дата звернення: 06.03.2021).

13. ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity. URL: www.iso.org/standard/44375.html (дата звернення: 06.03.2021).

References

1. Buriachok, V.L., Tolubko, V.B., Khoroshko, V.O. and Toliupa, S.V. (2015), *Informatsiina ta kiberbezpeka: sotsiotekhnichnyi aspekt* [Information and cybersecurity: sociotechnical aspect], textbook, DUT, Kyiv, Ukraine, 288 p.

2. Hirchenko, T.D., Chmeruk, H.H. and Semeniuk, I.M. (2020), "Ways to modernize the digital economy", *Infrastruktura rynku*, Iss. 41, pp. 25–30.

3. DSTU ISO/IEC 27032:2016 (ISO/IEC 27032:2012, IDT) (2016), *"*Information technologies. Methods of protection. Cybersecurity Guidelines", no. 448, available at: http://online.budstandart.com/ua/catalog/doc-page.html?Id_doc=69128. (access date March 06, 2021).

4. Dubov, D.V. and Ozhevan, M.A. (2011), *Kiberbezpeka: svitovi tendentsii ta vyklyky dlia Ukrainy* [Cybersecurity: global trends and challenges for Ukraine], NISS, Kyiv, Ukraine, 30 p.

5. Cabinet of Ministers of Ukraine (2018), Order of the Cabinet of Ministers of Ukraine "The concept of development of the digital economy and society of Ukraine for 2018-2020" of January 17, 2018 no. 67-p., available at: https://zakon.rada.gov.ua/laws/show/67-2018-%D1%80#Text. (access date March 06, 2021).

6. Liashenko, V.I. and Vyshnevskyi, O.S. (2018), *Tsyfrova modernizatsiya ekonomiky Ukrainy yak mozhlyvist proryvnoho rozvytku* [Digital modernization of Ukraine`s economy as an opportunity for breakthrough development], monograph, Kyiv, Ukraine, 252 p.

7. Nosatov, I.K. (2017), " Ways of information technology development in the context of strategic development of the national economy*", Naukovyy visnyk Khersonskoho derzhavnoho universytetu. Ekonomichni nauky,* Iss. 22, part 2, pp. 160–164.

8. Pantielieieva, N.M. (2019), "Cyber threats in the digital economy", *Finansovyi prostir*, no. 1, pp. 130–139.

9. Plikus, I.Y. (2019), "Digital economy: key trends in the world and prospects for Ukraine", *Molodyi vchenyi*, no. 12, pp. 470–476.

10. Decree of the President of Ukraine (2016), Cybersecurity strategy of Ukraine of March 15 no. 96, available at: https://zakon.rada.gov.ua/laws/show/96/2016#Text. (access date March 06, 2021).

11. "Cyber Security Strategy for Germany" (2016), available at: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/cyber-security-strategy-for-germany/@@download_version/5f3c65fe954c4d33ad6a9242cd5bb448/file_en (access date March 06, 2021).

12. "Cyber Security Strategy of the United Kingdom: safety, security and resilience in cyber space", available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/228841/7642.pdf. (access date March 06, 2021).

13. ISO/IEC 27032:2012 "*Information technology – Security techniques – Guidelines for cybersecurity"*, available at: www.iso.org/standard/44375.html. (access date March 06, 2021).